

Illumio + Netskope: Contain Machine-Speed Attacks From User to Workload

Control who can reach an application and what it can reach, so one compromise doesn't become a business-wide disaster

Frontier AI has given attackers machine speed. Now one compromised application can become a path across the business before manual response can catch up. Netskope and Illumio cut off that path from both sides — automatically. Netskope controls who can reach the application. Illumio controls what the application can reach.

Manual response falls behind

Frontier AI lets attackers find a weakness, exploit it, and move laterally to the next system in one automated run. An intrusion that once took days to become a breach now spreads from application to application in minutes. Attackers can weaponize a newly disclosed flaw in hours, but patching still takes weeks. Response that depends on tickets, approvals, and hand-edited rules can't keep up. AI didn't end security. It ended the comfort of slow response.

Secure access is still essential. But it answers only one question: who can connect to an application? Once a workload is compromised, the bigger question is what that workload can reach. Remote users and AI agents may still hold authorized sessions to a private application even after it becomes a risk, and access controls can't govern what the workload does after a connection is established. Containing the breach takes two coordinated controls: one that restricts user-to-application access and one that limits application-to-application communication. Netskope delivers the first. Illumio delivers the second. Together, they help keep one compromised application from becoming a business-wide disaster.

Coordinate access control and workload segmentation

Netskope One Private Access controls who can connect to a private application. Illumio Segmentation controls where that application can communicate if it's compromised. Each control is strong on its own. Connected, they help organizations contain an attack without waiting for responders to rewrite policies during an incident.

Here's how it works. The platforms share workload context, so access decisions reflect what Illumio knows about each workload. When a workload receives the configured quarantine label in Illumio, Netskope Cloud Exchange retrieves that context. Configured Netskope One Private Access policies then restrict user access to the application. At the same time, Illumio Segmentation limits the workload's permitted connections to other systems. Both responses run on policies you define in advance.

A coordinated response to a compromised application

Picture a business application that's been compromised. Two paths stay open. Users and AI agents may still be authorized to connect to it. And the workload itself may still have permitted connections to other systems. The coordinated response restricts both paths without broadly shutting down applications that weren't affected.

It works in three steps:

- 1. Mark the affected workload.** As part of the response workflow, the workload is assigned the configured quarantine label in Illumio. Existing segmentation policies restrict its permitted communications.
- 2. Adapt application access.** Netskope Cloud Exchange retrieves Illumio workload context. Configured Netskope One Private Access policies use the updated context to restrict access to the affected application.
- 3. Contain the disruption.** Access restrictions and workload segmentation limit exposure while responders investigate. Because both controls target only the affected application and workload, access to unaffected applications can continue. That way, the organization can avoid a broad shutdown.

Access updates follow the configured synchronization interval. Each platform enforces its own policies.

How coordinated containment protects your business

Limit the impact of compromise

Combine private application access controls with workload segmentation so that one compromised application stays one compromised application, not a breach that spreads across the business.

Keep access aligned with risk

Netskope uses current workload context from Illumio to decide who can reach each application. When an application is quarantined, access to it is restricted. As your applications change, access stays matched to each one's current risk.

Respond without rewriting policy during the attack

Set access and segmentation policies in advance. Then, when an incident hits, responders can quarantine a workload without waiting for new rules to be written and approved. Enforcement follows each platform's configured workflow and synchronization interval.

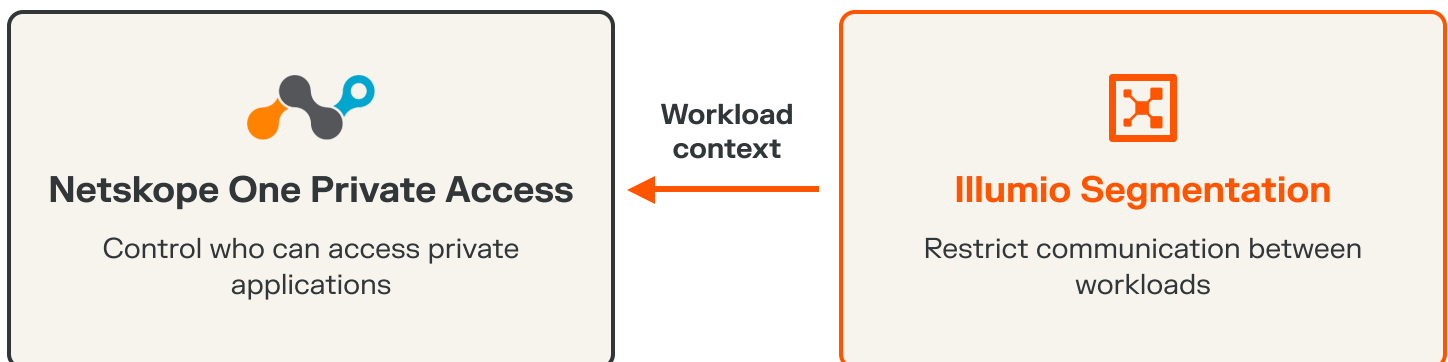


Figure 1. Illumio context informs Netskope access through Cloud Exchange.



Prepare containment policies before an incident

Containment works best when the hard decisions are made before an incident. Decide which applications users and agents can reach. Cut workload connections they don't need. Set how access will change when a workload is quarantined. Then test the coordinated policies so they're ready before you need them.

You can't stop breaches. You *can* stop disasters. Illumio and Netskope extend Zero Trust from the user connection to the workload, so one compromised application doesn't have to become a path across the business. Coordinate access control and segmentation before an incident, and you can contain the affected application, protect unaffected systems, and keep the business running — without manual policy changes while an attack is underway.

See the joint solution in action

Want to see how far an attacker could get from one compromised application? Ask your Illumio or Netskope representative for a demo. You'll see how Illumio and Netskope restrict access to a quarantined application, limit its connections to other workloads, and help contain disruption without a broad shutdown.

Learn more:

[illumio.com/
partners-tap/netskope](https://illumio.com/partners-tap/netskope)

About Illumio



Illumio is the leader in ransomware and breach containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by an AI security graph, our breach containment platform identifies and contains threats across hybrid multi-cloud environments — stopping the spread of attacks before they become disasters. Recognized as a Leader and Customer Favorite in The Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.

Copyright © 2026 Illumio, Inc. All rights reserved. Illumio® is a trademark or registered trademark of Illumio, Inc. or its affiliates in the U.S. and other countries. Third-party trademarks mentioned in this document are the property of their respective owners.